Amendments to the Claims

The listing of claims will replace all prior versions, and listings of claims in the application.

1. (Currently Amended) A file security system for restricting access to electronic files, said file security system comprising:

a key store being configured to store a plurality of cryptographic key pairs, each of the cryptographic key pairs includes a public key and a private key, at least one of the cryptographic key pairs pertaining to a predetermined time; and

an access manager operatively connected to said key store, said access manager being configured to determine whether the private key of the at least one of the cryptographic key pairs pertaining to the predetermined time is permitted to be provided to a requestor based on a current time,

wherein the requestor requires the private key of the at least one of the cryptographic key pairs pertaining to the predetermined time to access an encrypted header of a secured electronic file, and wherein a data portion of the secured electronic file was previously secured using a document key, and wherein the encrypted header includes the document key and access rules for the secured electronic file, and wherein the ~~document key~~ encrypted header was previously secured by the public key of the at least one of the cryptographic key pairs pertaining to the predetermined time.

2. (Previously Presented) The file security system as recited in claim 1, wherein said access manager provides the private key of the at least one of the

cryptographic key pairs pertaining to the predetermined time to the requestor if the predetermined time is less than or equal to the current time.

3. (Previously Presented) The file security system as recited in claim 1, wherein the requestor is a client module that operatively connects to say access manager over a network.

4. (Previously Presented) The file security system as recited in claim 1, wherein said file security system further comprises:

at least one client module, said at least one client module being configured to select the predetermined time and secure the electronic file, to generate to secured electronic file, using the public key of the at least one of the cryptographic key pairs pertaining to the predetermined time so as to provide a time-based access restriction to the electronic file.

5. (Previously Presented) The file security system as recited in claim 4, wherein said client module is further configured to unsecure the secured electronic file by acquiring the private key of the at least one of the cryptographic key pairs pertaining to the predetermined time from said key store, and then unsecuring the secured electronic file using the private key of the at least one of the cryptographic key pairs pertaining to the predetermined time.

6. (Currently Amended) A method for restricting access to an electronic document, said method comprising:

identifying an electronic document to be secured, the electronic document having at least a data portion that contains data, and a header portion that contains access rules for the electronic document;

determining whether a time-based access key is already available for a predetermined time, otherwise generating a time-based access key for the predetermined time;

securing the data portion of the electronic document through use of ~~the time-based access key and~~ a document key to produce a secured electronic document; ~~and~~

storing the document key in the header portion of the electronic document;

securing the header portion of the electronic document through the use of the time-based access key; and

storing the secured electronic document.

7. (Previously Presented) The method as recited in claim 6, wherein the time-based access key has an access time associated therewith.

8. (Previously Presented) The method as recited in claim 7, further comprising:

storing the time-based access key at a remote key store, wherein the time-based access key is subsequently retrievable from the remote key store when the current time is equal to or greater than the access time associated with the time-based access key.

9. (Previously Presented) The method as recited in claim 8, wherein said method is performed on a client machine that operatively receives the time-based access key from the remote key store over a network.

10. (Currently Amended) A method for restricting access to an electronic document, said method comprising:

identifying an electronic document to be secured, the electronic document having at least a data portion that contains data, and a header portion that contains access rules for the electronic document;

obtaining a document key;

encrypting the data portion of the electronic document using the document key to produce an encrypted data portion;

obtaining a time-based access key;

storing the document key in the header portion;

encrypting the ~~document key~~ header portion using the time-based access key to produce an encrypted ~~document key~~ header;

forming a secured electronic document from at least the encrypted data portion and the encrypted ~~document key~~ header; and

storing the secured electronic document.

11. (Previously Presented) The method as recited in claim 10, wherein the time-based access key is a public time-based access key.

12. (Previously Presented) The method as recited in claim 10, wherein the time-based access key has an access time associated therewith.

13. (Previously Presented) The method as recited in claim 12, wherein the time-based access key is available from a remote key store when the current time is equal to or greater than the access time associated with the time-based access key.

14. (Previously Presented) The method as recited in claim 13, wherein

the access time is a day of a year, and

the time-based access key is unique for each day of the year.

15. (Previously Presented) The method as recited in claim 13, wherein said method is performed on a client machine that operatively receives the time-based access key from the remote key store over a network.

16. (Currently Amended) A method for accessing a secured electronic document by a requester, the secured electronic document having at least ~~a~~ an encrypted header portion and an encrypted data portion, said method comprising:

obtaining a time-based access key;

~~obtaining an encrypted document key from the header portion of the secured electronic document;~~

decrypting the encrypted header portion ~~document key~~ using the time-based access key to produce a document key and access rules for the secured electronic document;

decrypting the encrypted data portion of the secured electronic document using the document key to produce a data portion; and

supplying the data portion to the requestor.

17. (Previously Presented) The method as recited in claim 16, wherein the time-based access key is identified by an indicator within a header portion of the secured electronic document.

18. (Previously Presented) The method as recited in claim 16, wherein the time-based access key is a private time-based access key.

19. (Previously Presented) The method as recited in claim 18, wherein the time-based access key being obtained is acquired from a server.

20. (Previously Presented) The method as recited in claim 16, wherein said obtaining of the time-based access key is dependent on the current time.

21. (Previously Presented) The method as recited in claim 16, wherein the time-based access key is associated with an access time, and wherein said obtaining of

the time-based access key is permitted when the current time is greater than or equal to the access time.

22. (Previously Presented) The method as recited in claim 21, wherein, if permitted, during said obtaining step the time-based access key is obtained from a server.

23-25. (Cancelled)

26. (Currently Amended) A computer readable medium including at least computer program code for restricting access to an electronic document, said computer readable medium comprising:

computer program code for identifying an electronic document to be secured, the electronic document having at least a data portion that contains data, and a header portion that contains access rules for the electronic document;

computer program code for determining whether a time-based access key is already available for a predetermined time, otherwise generating a time-based access key for the predetermined time;

computer program code for securing the data portion of the electronic document through use of ~~the time-based access key and~~ a document key to produce a secured electronic document; ~~and~~

computer program code for storing the document key in the header portion of the electronic document;

computer program code for securing the header portion of the electronic document through the use of the time-based access key; and

computer program code for storing the secured electronic document.

27. (Previously Presented) The computer readable medium as recited in claim 26, wherein the time-based access key has an access time associated therewith.

28. (Previously Presented) The computer readable medium as recited in claim 27,

wherein said computer readable medium further comprises:

computer program code for storing the time-based access key at a remote key store, and

wherein the time-based access key is subsequently retrievable from the remote key store when the current time is greater than or equal to the access time associated with the time-based access key.

29. (Currently Amended) A computer-readable medium containing instructions for controlling at least one processor by a method comprising:

identifying an electronic document to be secured, the electronic document having at least a data portion that contains data, and a header portion that contains access rules for the electronic document;

determining whether a time-based access key is already available for a predetermined time, otherwise generating a time-based access key for the predetermined time;

securing the data portion of the electronic document through use of ~~the time-based access key and~~ a document key to produce a secured electronic document; ~~and~~

storing the document key in the header portion of the electronic document;

securing the header portion of the electronic document through the use of the time-based access key; and

storing the secured electronic document.

30. (Currently Amended) A computer-readable medium containing instructions that, when executed by a processor, causes the processor to:

identify an electronic document to be secured, the electronic document having at least a data portion that contains data, and a header portion that contains access rules for the electronic document;

obtain a document key;

encrypt the data portion of the electronic document using the document key to produce an encrypted data portion;

obtain a time-based access key;

store the document key in the header portion;

encrypt the ~~document key~~ header portion using the time-based access key to produce an encrypted ~~document key~~ header;

form a secured electronic document from at least the encrypted data portion and the encrypted ~~document key~~ header; and

store the secured electronic document.

31. (Currently Amended) A computer-readable medium containing instructions that, when executed by a processor, causes the processor to:

obtain a time-based access key;

~~obtain an encrypted document key from a header portion of the secured electronic document;~~

decrypt ~~the~~ an encrypted ~~document key~~ header portion of a secured electronic document using the time-based access key to produce a document key and access rules for the secured electronic document;

decrypt an encrypted data portion of the secured electronic document using the document key to produce a data portion; and

supply the data portion to the requestor.